

Vertrag über Auftragsverarbeitung nach Art. 28 DSGVO

Stand: 13.04.2026

zwischen

Vent.Net Web-Software Andreas Vent-Schmidt

Kieselbach 7c

04746 Hartha

Deutschland

Telefon: +49 34321 63 59 77

E-Mail: xrechnung@vent.net

- nachfolgend „Auftragsverarbeiter“ -

und

dem jeweiligen Kunden der API-Nutzung von XInvoice

- nachfolgend „Verantwortlicher“ -

wird folgender Vertrag geschlossen:

1. Gegenstand des Vertrags

1. Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen im Zusammenhang mit dem Dienst `XInvoice`, insbesondere im Bereich der Verarbeitung, Validierung, Erzeugung, Bereitstellung und Verwaltung elektronischer Rechnungsdaten über Web-Portal und API.
2. Soweit der Auftragsverarbeiter dabei personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet, erfolgt diese Verarbeitung ausschließlich nach Maßgabe dieses Vertrags.

2. Dauer

1. Dieser Vertrag gilt ab Annahme durch den Verantwortlichen.
2. Er läuft für die Dauer der Nutzung der API oder sonstiger verarbeitungsrelevanter Leistungen des Auftragsverarbeiters.
3. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.
4. Mit Beendigung des Hauptvertrags endet auch dieser Vertrag, sofern keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

3. Art und Zweck der Verarbeitung

1. Die Verarbeitung erfolgt zur technischen Bereitstellung des Dienstes `xInvoice` und umfasst insbesondere:
 - Entgegennahme strukturierter Rechnungsdaten
 - Validierung von Rechnungsdaten und Rechnungsdokumenten
 - Erzeugung strukturierter Rechnungsdokumente
 - technische Speicherung und Bereitstellung von Ergebnissen
 - Download- und Abruffunktionen
 - Fehleranalyse, Protokollierung und technische Unterstützung
 - Sicherheits- und Missbrauchsschutz
2. Die Verarbeitung dient ausschließlich den vom Verantwortlichen veranlassten Zwecken im Rahmen der Nutzung des Dienstes.

4. Art der personenbezogenen Daten und Kategorien betroffener Personen

4.1 Kategorien personenbezogener Daten

Je nach Nutzung des Dienstes können insbesondere folgende Daten verarbeitet werden:

- Stammdaten
- Kontaktdaten
- Adressdaten
- E-Mail-Adressen
- Telefonnummern
- Rechnungs- und Bestelldaten
- Leistungs- und Positionsdaten
- Zahlungs- und Abrechnungsdaten
- Steuer- und Identifikationsdaten
- Kommunikationsinhalte
- technische Nutzungs- und Protokolldaten

4.2 Kategorien betroffener Personen

Von der Verarbeitung können insbesondere betroffen sein:

- Ansprechpartner des Verantwortlichen
- Mitarbeiter des Verantwortlichen
- Kunden, Lieferanten oder Geschäftspartner des Verantwortlichen
- Rechnungsempfänger
- sonstige natürliche Personen, deren Daten in übermittelten Rechnungs- oder Geschäftsdaten enthalten sind

5. Pflichten des Verantwortlichen

1. Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Rechte betroffener Personen verantwortlich.

2. Der Verantwortliche hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er Fehler oder Unregelmäßigkeiten im Zusammenhang mit datenschutzrechtlichen Anforderungen feststellt.
3. Der Verantwortliche ist verpflichtet, dem Auftragsverarbeiter nur solche Daten zu übermitteln, deren Verarbeitung datenschutzrechtlich zulässig ist.
4. Weisungen des Verantwortlichen sind grundsätzlich in dokumentierter Form zu erteilen.

6. Weisungsrecht

1. Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch Unionsrecht oder das Recht der Mitgliedstaaten zur Verarbeitung verpflichtet ist.
2. Mündliche Weisungen sind unverzüglich in Textform zu bestätigen.
3. Ist der Auftragsverarbeiter der Auffassung, dass eine Weisung gegen geltendes Datenschutzrecht verstößt, wird er den Verantwortlichen hierauf unverzüglich hinweisen.

7. Vertraulichkeit

1. Der Auftragsverarbeiter stellt sicher, dass alle zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
2. Der Zugriff auf personenbezogene Daten erfolgt nur im erforderlichen Umfang nach dem Need-to-know-Prinzip.

8. Technische und organisatorische Maßnahmen

1. Der Auftragsverarbeiter trifft angemessene technische und organisatorische Maßnahmen im Sinne von Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

2. Dazu gehören insbesondere Maßnahmen in den folgenden Bereichen:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Verfügbarkeitskontrolle
- Belastbarkeit und Wiederherstellbarkeit von Systemen
- Trennung von Daten unterschiedlicher Kunden
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der Maßnahmen

3. Der Auftragsverarbeiter ist berechtigt, technische und organisatorische Maßnahmen weiterzuentwickeln, sofern das Schutzniveau insgesamt nicht verschlechtert wird.

9. Unterstützung des Verantwortlichen

1. Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der Pflichten in Bezug auf:

- Betroffenenrechte
- Sicherheit der Verarbeitung
- Meldung von Verletzungen des Schutzes personenbezogener Daten
- Datenschutz-Folgenabschätzungen
- Konsultationen mit Aufsichtsbehörden

2. Soweit die Unterstützung nicht bereits von der vertraglichen Leistung umfasst ist, kann sie gesondert vergütet werden.

10. Meldung von Datenschutzvorfällen

1. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Daten des Verantwortlichen betrifft.
2. Die Mitteilung erfolgt mit den verfügbaren Informationen, die der Verantwortliche zur Erfüllung seiner gesetzlichen Pflichten benötigt.

11. Unterauftragsverarbeiter

1. Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen, soweit dies zur Leistungserbringung erforderlich ist.
2. Der Auftragsverarbeiter wird den Verantwortlichen über beabsichtigte wesentliche Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern informieren.
3. Der Verantwortliche kann einer solchen Änderung aus wichtigem datenschutzrechtlichem Grund widersprechen.
4. Der Auftragsverarbeiter wird mit Unterauftragsverarbeitern vertragliche Regelungen treffen, die den Anforderungen des Art. 28 DSGVO entsprechen.

12. Nachweismöglichkeiten und Audits

1. Der Auftragsverarbeiter stellt dem Verantwortlichen auf Anfrage geeignete Informationen zum Nachweis der Einhaltung der in diesem Vertrag niedergelegten Pflichten zur Verfügung.
2. Soweit erforderlich und verhältnismäßig, kann der Verantwortliche nach angemessener Vorankündigung Audits oder Prüfungen durchführen oder durch einen zur Verschwiegenheit

verpflichteten Prüfer durchführen lassen.

3. Audits haben den Geschäftsbetrieb des Auftragsverarbeiters nicht unangemessen zu beeinträchtigen und sind auf das erforderliche Maß zu beschränken.
4. Der Auftragsverarbeiter kann die Durchführung eines Audits von angemessenen Sicherheits- und Vertraulichkeitsanforderungen abhängig machen.

13. Rückgabe und Löschung

1. Nach Beendigung der vertraglichen Leistungen wird der Auftragsverarbeiter personenbezogene Daten des Verantwortlichen nach dessen Wahl löschen oder zurückgeben, sofern keine gesetzliche Pflicht zur weiteren Speicherung besteht.
2. Gesetzliche Aufbewahrungspflichten bleiben unberührt.
3. Nachweise über die ordnungsgemäße Löschung oder Rückgabe können vom Verantwortlichen angefordert werden.

14. Drittlandverarbeitung

1. Eine Verarbeitung in einem Drittland erfolgt nur, wenn die gesetzlichen Voraussetzungen der DSGVO eingehalten sind.
2. Soweit Unterauftragsverarbeiter oder technische Dienste in Drittländern eingesetzt werden, stellt der Auftragsverarbeiter sicher, dass geeignete Garantien bestehen.

15. Haftung

1. Die Haftung der Parteien richtet sich nach den gesetzlichen Vorschriften sowie nach den Vereinbarungen des Hauptvertrags, soweit diese mit dem Datenschutzrecht vereinbar sind.
2. Zwingende gesetzliche Haftungsregelungen, insbesondere aus der DSGVO, bleiben unberührt.

16. Schlussbestimmungen

1. Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform, soweit nicht eine strengere Form gesetzlich vorgeschrieben ist.
 2. Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.
 3. Im Übrigen gelten die Regelungen des Hauptvertrags.
-

Anlage 1: Beschreibung der Verarbeitung

1. Gegenstand

Bereitstellung und Betrieb des Dienstes *xInvoice* zur Verarbeitung, Validierung, Erzeugung und Bereitstellung elektronischer Rechnungsdaten und strukturierter Rechnungsdokumente.

2. Zweck

Technische Durchführung der vom Verantwortlichen veranlassten Rechnungsverarbeitung und Bereitstellung der hierzu vereinbarten Funktionen.

3. Art der Verarbeitung

- Erheben
- Erfassen
- Strukturieren
- Speichern
- Anpassen
- Auslesen
- Verwenden

- Übermitteln innerhalb der vereinbarten Systemumgebung
- Bereitstellen zum Abruf
- Löschen

4. Betroffene Datenkategorien

- Namen
- Kontaktdaten
- Adressdaten
- Rechnungsdaten
- Leistungsdaten
- Zahlungsdaten
- Steuerdaten
- Kommunikationsdaten
- technische Metadaten

5. Betroffene Personengruppen

- Ansprechpartner
- Mitarbeiter
- Kunden
- Rechnungsempfänger
- sonstige in Rechnungsdaten enthaltene natürliche Personen

Anlage 2: Technische und organisatorische Maßnahmen

Der Auftragsverarbeiter setzt angemessene technische und organisatorische Maßnahmen um, insbesondere:

- rollenbasierte Zugriffsbeschränkungen
- Authentifizierungsschutz
- sichere Passwortverarbeitung
- Protokollierung sicherheitsrelevanter Ereignisse
- Trennung von Kundendaten
- Absicherung von Schnittstellen
- Maßnahmen zur Sicherstellung von Verfügbarkeit und Wiederherstellbarkeit
- Verfahren zur Erkennung und Behandlung von Sicherheitsvorfällen
- regelmäßige Pflege und Aktualisierung der eingesetzten Systeme

Version: v2026-04-13